MATH 521A: Abstract Algebra

Homework 7 Solutions

1. List all polynomials in $\mathbb{Z}_3[x]$ of degree at most 1. Determine which are units and which are zero divisors.

   There are nine[1]: $a_1(x) = 0 + 0x, a_2(x) = 0 + x, a_3(x) = 0 + 2x, a_4(x) = 1 + 0x, a_5(x) = 1 + x, a_6(x) = 1 + 2x, a_7(x) = 2 + 0x, a_8(x) = 2 + x, a_9(x) = 2 + 2x$. There are no zero divisors, as $\mathbb{Z}_3[x]$ is an integral domain (since $\mathbb{Z}_3$ is). By a theorem from class, only $a_4(x)$ and $a_7(x)$ are units, each of which is its own reciprocal.

2. List all polynomials in $\mathbb{Z}_4[x]$ of degree at most 1. Determine which are units and which are zero divisors.

   There are sixteen: $a_1(x) = 0 + 0x, a_2(x) = 0 + x, a_3(x) = 0 + 2x, a_4(x) = 1 + 0x, a_5(x) = 1 + x, a_6(x) = 1 + 2x, a_7(x) = 2 + 0x, a_8(x) = 2 + x, a_9(x) = 2 + 2x, a_{10}(x) = 0 + 3x, a_{11}(x) = 1 + 3x, a_{12}(x) = 2 + 3x, a_{13} = 3 + 3x, a_{14} = 3 + 2x, a_{15} = 3 + x, a_{16} = 3 + 0x$. There are three zero divisors, namely $a_3(x), a_7(x), a_9(x)$; multiply any two of them together to get 0. $a_4(x), a_6(x), a_{14}(x), a_{16}(x)$ are each their own reciprocals; these are the only units. Note: in a unit of degree 1, the leading coefficient must be a zero divisor, which in this ring is just 2.

3. Let R be a commutative ring with identity. Define $f : R[x] \to R$ via $f : a_0 + a_1x + \cdots + a_nx^n \mapsto a_0$. Prove that f is a (ring) homomorphism and find its kernel and image.

   We have $f(a_0 + a_1x + \cdots + a_nx^n + a_0' + a_1'x + \cdots + a_n'x^n) = f((a_0 + a_0') + (a_1 + a_1')x + \cdots + (a_n + a_n')x^n) = a_0 + a_0' = f(a_0 + a_1x + \cdots + a_nx^n) + f(a_0' + a_1'x + \cdots + a_n'x^n)$, and $f((a_0 + a_1x + \cdots + a_nx^n)(a_0' + a_1'x + \cdots + a_n'x^n)) = f(a_0a_0' + \text{ higher order terms}) = a_0a_0' = f(a_0 + a_1x + \cdots + a_nx^n)f(a_0' + a_1'x + \cdots + a_n'x^n)$.

   The kernel is the set of those polynomials with zero constant term, equivalently $xR[x]$. We now prove that the image is R; let $a \in R$, then set $p(x) = a$, a constant polynomial. We have $f(p) = a$.

4. Let R be a commutative ring with identity. Let $a \in R$ be nilpotent. Prove that $1_R - ax$ is a unit in $R[x]$.

   Since a is nilpotent, there is some $n \in \mathbb{N}$ so that $a^n = 0$. We calculate a product of two nonzero elements: $(1_R - ax)(1_R + ax + a^2x^2 + \cdots + a^{n-1}x^{n-1}) = 1_R - a^nx^n = 1_R$.

5. Working in $\mathbb{Z}_3[x]$, find $\gcd(a(x), b(x))$, for $a(x) = x^3 + x^2 + 2x + 2$, $b(x) = x^4 + 2x^2 + x + 1$.

$$x^4 + 2x^2 + x + 1 = (x^3 + x^2 + 2x + 2)(x - 1) + (x^2 + x)$$
$$x^3 + x^2 + 2x + 2 = (x^2 + x)(x) + (2x + 2)$$
$$x^2 + x = (2x + 2)(2x) + 0$$

   Hence the gcd is the monic $\mathbb{Z}_3$-multiple of $2x + 2$, namely $2(2x + 2) = x + 1$.

[1] Assuming we take the degree of polynomial 0 to be $-\infty$. If we join our book's author and say that this degree is undefined, then remove that polynomial from the list.

6. Working in $\mathbb{Q}[x]$, find $\gcd(a(x), b(x))$, for $a(x) = 3x^2 + 2$, $b(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$.

$$\begin{aligned}
4x^4 + 2x^3 + 6x^2 + 4x + 5 &= \left(3x^2 + 2\right) \cdot \left(\tfrac{4}{3}x^2 + \tfrac{2}{3}x + \tfrac{10}{9}\right) + \left(\tfrac{8}{3}x + \tfrac{25}{9}\right) \\
3x^2 + 2 &= \left(\tfrac{8}{3}x + \tfrac{25}{9}\right) \cdot \left(\tfrac{9}{8}x - \tfrac{75}{64}\right) + \tfrac{1009}{192} \\
\tfrac{8}{3}x + \tfrac{25}{9} &= \tfrac{1009}{192} \cdot \left(\tfrac{512}{1009}x + \tfrac{1600}{3027}\right) + 0
\end{aligned}$$

Hence the gcd is the monic $\mathbb{Q}$-multiple of $\frac{1009}{192}$, namely 1.

7. Working in $\mathbb{Z}_7[x]$, find $\gcd(a(x), b(x))$, for $a(x) = 3x^2 + 2$, $b(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$.

$$\begin{aligned}
4x^4 + 2x^3 + 6x^2 + 4x + 5 &= (3x^2 + 2)(6x^2 + 3x + 5) + (5x + 2) \\
3x^2 + 2 &= (5x + 2)(2x + 2) + (5) \\
5x + 2 &= (5)(x + 6) + 0
\end{aligned}$$

Hence the gcd is the monic $\mathbb{Z}_7$-multiple of 5, namely $3(5) = 1$.

8. Working in $\mathbb{Z}_7[x]$, let $a(x) = 3x^2 + 2$, $b(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$. Find $u(x), v(x)$ such that $\gcd(a(x), b(x)) = a(x)u(x) + b(x)v(x)$.

$$\begin{aligned}
5 &= (3x^2 + 2) + (5x + 2)(-2x - 2) \\
&= (3x^2 + 2) + \left(4x^4 + 2x^3 + 6x^2 + 4x + 5) + (3x^2 + 2)(-6x^2 - 3x - 5)\right)(-2x - 2) \\
&= (3x^2 + 2)(1 + (-6x^2 - 3x - 5)(-2x - 2)) + (4x^4 + 2x^3 + 6x^2 + 4x + 5)(-2x - 2) \\
&= (3x^2 + 2)(5x^3 + 4x^2 + 2x + 4) + (4x^4 + 2x^3 + 6x^2 + 4x + 5)(5x + 5)
\end{aligned}$$

We now multiply both sides by 3 to get $u(x) = 3(5x^3 + 4x^2 + 2x + 4) = x^3 + 5x^2 + 6x + 5$ and $v(x) = 3(5x + 5) = x + 1$.

9. Working in $\mathbb{Z}_{10}[x]$, find two degree-1 polynomials whose product is $x + 7$.

We have $(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$. For this to be $x + 7$, we must have $ac = 0$. Let's try $a = 2, c = 5$. Then we have to solve the modular system of equations $\{2d + 5b = 1, bd = 7\}$. Luckily there aren't too many combinations to try until we find $b = 9, d = 3$. Hence $(2x + 9)(5x + 3) = x + 7$.